IJREB

ISSN 2321-743X

International Journal of Research in

Engineering and Bioscience

Volume 2 (Issue 4) Pages (01-08)

Journal home page: www.ijreb.org

MULTI AUTHORITY ATTRIBUTE BASED ENCRYPTION IN PROXY SERVER

Sreelekshmi.P.G and Thara Krishnan.R

*Department of Computer Science and Engineering, Narayana Guru College of Engineering, Manjalumoodu, K.K Dist, Tamil Nadu

ABSTRACT

A Decentralized Attribute Based Encryption (ABE) is a variant of multi-authority ABE scheme where each authority can issue secret keys to the user independently without central authority. We proposed a privacy-preserving decentralized ABE scheme to protect the user's privacy. In our scheme, all the user's secret keys are tied to his identifier to resist the collusion attacks while the multiple authorities cannot know anything about the user's identifier. The concept of proxy re-encryption (PRE) in which a proxy can transform, without seeing the plain text, a cipher text encrypted under one key into an encryption of the same plain text under another key. This project deals with the case of unidirectional PRE schemes. This will ensure both authentication and confidentiality.

KEYWORDS: Proxy re-encryption, Multi authority, cipher-text, plain text.

IJREB

ISSN 2321-743X

International Journal of Research in

Engineering and Bioscience

Volume 2 (Issue 4) Pages (01-08)

Journal home page: www.ijreb.org

INTRODUCTION

This paper addresses secure file exchange between users logged in to an organization. In common normal encryption and decryption techniques are employed. Here we are doing attribute based encryption. Being different from the traditional access control schemes, attribute-based access control are the schemes that allow users to be validated by the descriptive attributes instead of their unique identities. Furthermore, a user can share his data by specifying an access structure so that all the users whose attributes satisfy it can access the data without knowing their identities. Therefore, attribute-based access control schemes are efficient primitives to share data with multiple users without knowing their identities.

In many situations, [1] when a user encrypts sensitive data, it is imperative that she establish a specific access control policy on who can decrypt this data. It can be crucial that the person in possession of the secret data be able to choose an access policy based on specific knowledge of the underlying data. Furthermore, this person may not know the exact identities of all other people who should be able to access the data, but rather she may only have a way to describe them in terms of descriptive attributes.

In an open communication environment, such as the Internet, sensitive data must be encrypted prior to being transmitted. To achieve this, encryption schemes can be employed to protect the confidentiality of the sensitive data. Nevertheless, traditional encryption schemes cannot express a complex access policy, and additionally, the sender must know all the public keys of the receivers. Attribute-based encryption (ABE) is a more efficient encryption scheme and it can express a complex access structure. In an ABE scheme, both the user's secret keys and the cipher text are labelled with sets of attributes. The encrypter can encrypt a message under a set of attributes. Prior to decrypting the cipher text, the receiver must obtain the secret (attribute) keys from the central authority (CA). The receiver can decrypt the cipher text and obtain the data if and only if there is a match between his secret keys and the attributes listed in the cipher text.

There are two kinds of ABE schemes:

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (01-08)
IJREB
Journal home page: www.ijreb.org

Key-Policy ABE (KP-ABE): In these schemes, the secret keys are associated with an access structure, while the cipher text is labelled with a set of attributes. Cipher text-Policy ABE (CP-ABE): In these schemes, the cipher text is associated with an access structure, while the secret keys are labelled with a set of attributes.

An access structure is employed to control users from accessing the protected resource in systems where users need to cooperate with multiple parties. Sahai and Waters proposed an ABE scheme [2] for fine-grained access policy where any monotonic access structure can be expressed by an access tree. In an access tree, there is a tree access structure where interior nodes consist of AND and OR gates and the leaves consist of the attributes. Each interior node x of the tree specifies a threshold gate (kx, nx), where nx is the number of the children of x and $kx \leq nx$. Thereafter, when kx = nx, the gate is an AND gate. When kx = 1, the gate is an OR gate. If a set of attributes satisfies the tree access structure, the corresponding secret keys can be used to reconstruct the secret embedded in the vertex of the tree.

An ABE scheme should be secure against the collusion attacks [3], namely no group of users can combine their secret keys to decrypt the cipher text which none of them can decrypt by himself. The most common technique to prevent collusion attacks is randomization. The central authority randomizes the user's secret keys by selecting random numbers [4] or random polynomials [3], [5]. ABE has been used as a building block to express flexible access structures in practical systems, such as distributed systems [6], data outsourcing systems [7] and cloud computing [8].

RELATED WORKS

There is a trend for sensitive user data to be stored by third parties on the Internet. For example, personal email, data, and personal preferences are stored on web portal sites such as Google and Yahoo. The attack correlation center, dshield.org, presents aggregated views of attacks on the Internet, but stores intrusion reports individually submitted by users [2]. Given the variety, amount, and importance of information stored at these sites, there is cause for concern that personal data will be compromised. This worry is escalated by the

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (01-08)
IJREB
Journal home page: www.ijreb.org

surge in recent attacks and legal pressure faced by such services.

One method for alleviating some of these problems is to store data in encrypted form. Thus, if the storage is compromised the amount of information loss will be limited. One disadvantage of encrypting data is that it severely limits the ability of users to selectively share their encrypted data at a fine-grained level. Suppose a particular user wants to grant decryption access to a party to all of its Internet traffic logs for all entries on a particular range of dates that had a source IP address from a particular subnet.

Encryption is the cryptographic primitive which provides confidentiality to digital communications. In a traditional public key encryption scheme, a message is encrypted with the public key of the intended receiver, who is the only person able to decrypt. This level of confidentiality is enough for many real-life applications, including e-mail. However, new situations requiring different cryptographic functionalities appear constantly. An attribute based encryption scheme (ABE), in contrast, is a scheme in which each user is identified by a set of attributes, and some function of those attributes is used to determine decryption ability for each cipher text.

PROPOSED DESCRIPTION

In the proposed method, shows the secure file exchange between users logged in to an organization. The exchange may be broadcast, groupcast or between individuals.

This exchange of files is controlled by the proxy server. When a user logged in to the organization proxy creates a key pair to the user. The user is not aware of the key created.

The plain text a user wants to send to another user is encrypted by the proxy using the key created for the user. The encryption is carried out at the users site .The encrypted data is send to the concerned receiver through proxy's site. In the proxy's site, proxy decrypts the data and obtains the plaintext. It again encrypts the data using another key assigned for receiver and sends the encrypted data to receiver. Before decryption the receiver should obtain a secret key from the proxy. If the attributes in the secret key obtained by the receiver from the proxy matches with that of attributes listed in the ciphertext, then only the decryption is carried out by the proxy at the receiver side. The first encryption is based on

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (01-08)
IJREB
Journal home page: www.ijreb.org

AES encryption and second one is Attribute Based Encryption. ABE allow users to be validated by the descriptive attributes instead of their unique identities.ABE is associated with access structures [9].

The concept of proxy re-encryption (PRE) in which a proxy can transform, without seeing the plain text, a cipher text encrypted under one key into an encryption of the same plain text under another key. Their construction is bidirectional in that any information to translate cipher text from Alice to Bob can also be used to translate from Bob to Alice. Notably, each authority can join or leave the system freely without the need of reinitializing the system and there is central authority.

Here deals with the case of unidirectional PRE schemes and answers the question of how to secure them against chosen-cipher text attacks while keeping them efficient. While sending a message from A to B, there is a possibility for the plaintext to undergo a Brute Force attack or any other cryptanalytic attack, in the proxy server. To avoid such situations, here we are applying both symmetric and asymmetric encryption algorithms. This will ensure both authentication and confidentiality.

For key generation an algorithm called Blind Key Generation is used. It involves authorities and users. Commit and decommit operations are carried out. If the decommit operation can decommit the committed operation, ie if the decommit operation returns the value 1, then secret key is issued to the user else an error message is displayed. The algorithm BlindKeyGen should satisfy the following two properties: leak-freeness and selective-failure blindness [10], [11].

ANALYSIS

In the existing system only one encryption and decryption is carried out. The encryption and decryption is handled by the proxy but it was not carried out in the proxy's site. The file exchange is bi-directional. Their construction is bidirectional in that any information to translate cipher text from Alice to Bob can also be used to translate from Bob to Alice. Notably, each authority can join or leave the system freely without the need of reinitializing the system and there is central authority.

In the proposed system, double encryption and decryption is carried out. Both of this is handled by the proxy. One encryption and decryption is carried out in senders and

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (01-08)
IJREB
Journal home page: www.ijreb.org

receivers site and another encryption and decryption is carried out in proxy's site. The concept of proxy re-encryption (PRE) in which a proxy can transform, without seeing the plain text, a cipher text encrypted under one key into an encryption of the same plain text under another key. This system deals with the case of unidirectional PRE schemes.

This system provides two software packages. First, the client module which is manually operated by different users. This module ensures a secure file transfer channel and encrypted chatting facility. In addition it provides service access. Second, the proxy module, which is fully automated and consists of two components: the client monitoring system, which monitors online clients, their public key status, traffic and any malicious activities. And the security module, which manages encryption and decryption in proxy servers, their key strength and encryption and decryption rate.

This paper ensures a 2-level security or confidentiality. The first level is achieved at the senders side where the plain text undergoes double encryption (symmetric and asymmetric) and the second level is achieved at the proxy server side where first the plain text is decrypted using the senders public key and then re-encrypted using the receivers public key.

CONCLUSION

This paper deals with the case of unidirectional PRE schemes and answers the question of how to secure them against chosen-cipher text attacks while keeping them efficient. While sending a message from A to B, there is a possibility for the plaintext to undergo a Brute Force attack or any other cryptanalytic attack, in the proxy server. To avoid such situations, here we are applying both symmetric and asymmetric encryption algorithms. This will ensure both authentication and confidentiality. In addition this paper ensures a 20% of cost reduction.

REFERENCES

1. J. Bettencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute-based encryption," in Proceedings: IEEE Symposium on Security and Privacy (S & P'07), (Oakland, California, USA), pp. 321–34, IEEE, May 20-23 2007.

2. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted

IJREB

ISSN 2321-743X

International Journal of Research in

Engineering and Bioscience

Volume 2 (Issue 4) Pages (01-08)

Journal home page: www.ijreb.org

data," in Proceedings: ACM Conference on Computer and Communications

Security-CCS'06 (A. Juels, R. N. Wright, and S. D. C. di Vimercati, eds.), (Alexandria, VA, USA), pp. 89–98, ACM, October 30- November 3 2006.

3. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proceedings: Advances in Cryptology - EUROCRYPT'05 (R. Cramer, ed.), vol. 3494 of Lecture Notes in Computer Science, (Aarhus, Denmark), pp. 457–473, Springer, May 22-26 2005.

4.R. Ostrovsky, A. Sahai, and B. Waters, "Attribute- based encryption with non-monotonic access structures," in Proceedings: ACM Conference on Computer and Communications Security-CCS'07 (P. Ning, S. D. C. di Vimercati, and P. F. Syverson, eds.), (Alexandria,Virginia, USA), pp. 195–203, ACM, October 28-31 2007.

5. M. Chase, "Multi-authority attribute based encryption," in Proceedings: Theory of Cryptography Conference-TCC'07 (S. P. Vadhan, ed.), vol. 4392 of Lecture Notes in Computer Science, (Amsterdam, The Netherlands), pp. 515–534, Springer, February 21-24 2007.

6. S. Yu, K. Ren, and W. Lou, "FDAC: Toward fine-grained data access control in wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 4, pp. 673–686, 2011.

7. J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214–1221 2011.

8. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proceedings: IEEE International Conference on Computer Communications-INFOCOM'10, (San Diego, CA, USA), pp. 534– 542, IEEE, March 15-19 2010.

9. R. Ostrovsky, A. Sahai, and B. Waters, "Attribute- based encryption with non-monotonic access structures," in Proceedings: ACM Conference on

IJREB

ISSN 2321-743X

International Journal of Research in

Engineering and Bioscience

Volume 2 (Issue 4) Pages (01-08)

Journal home page: www.ijreb.org

Computer and Communications Security-CCS'07 (P. Ning, S. D. C. di Vimercati, and P. F. Syverson, eds.), (Alexandria, Virginia, USA), pp. 195–203, ACM, October 28-31 2007.

10. J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and anonymous identity-based encryption and authorized private searches on public key encrypted data," in Proceedings: Public Key Cryptography - PKC'09 (S. Jarecki and G. Tsudik, eds.), vol. 5443 of Lecture Notes in Computer Scienc, (Irvine, CA, USA), pp. 196–214, Springer, March 18-20 2009.

11. M. Green and S. Hohenberger, "Blind identity-based encryption and simulatable oblivious transfer," in Proceedings: Advances in Cryptology-ASIACRYPT'07 (K. Kurosawa, ed.), vol. 4833 of Lecture Notes in Computer Science, (Kuching, Malaysia), pp. 265–282, Springer, December 2-6 2007.